УДК 01.05.02; 05.13.06; 05.13.21

Доц. Т. Є. Рак, д-р техн. наук; Ю.О. Борзов -
Львівський Державний університет безпеки життєдіяльності

ЛІНІЙНІ ФОРМИ З ЕЛЕМЕНТАМИ АЛГОРИТМУ RSA І ДОДАТКОВЕ ЗАШУМЛЕННЯ В ЗАХИСТІ ПІВТОНОВИХ ЗОБРАЖЕНЬ

Розглянуто проблеми захисту зображень від несанкціонованого доступу. Сформульовано вимоги до методів шифрування у випадку їх використання стосовно зображень – повна зашумленість зашифрованого зображення. Описано використання елементів алгоритму RSA і лінійних форм для використання при шифруванні – дешифруванні зображень при наявності додаткового зашумлення. Запропонована модифікація базового алгоритму RSA може застосовуватись для шифрування як для півтонових, так і для кольорових зображень. Стійкість до несанкціонованого дешифрування запропонованого алгоритму забезпечується стійкістю базового алгоритму RSA з додатковою стійкістю, яка надається використанням лінійних форм.

Ключові слова: шифрування, дешифрування, алгоритм RSA, лінійна форма.

Вступ

Зображення — відтворення виду, форми і кольору предмета світловими променями, що пройшли оптичну систему з центрованих сферичних поверхонь, які мають одну загальну оптичну вісь. Якщо зображення предмета утворено перетинанням самих променів, то воно називається дійсним, якщо їхнім продовженням — уявним. При цьому можливі такі випадки: при розташуванні предмета за подвійною фокусною відстанню від системи його зображення, розташоване за першим фокусом у просторі зображень, буде дійсним, зменшеним і зворотним; при розташуванні предмета на подвійній фокусній відстані від системи його зображення, розташоване в просторі зображень також на подвійній фокусній відстані від системи, буде дійсним, рівним самому предмету і зворотним; якщо предмет розташований між першим і другим фокусами, його зображення, одержуване в просторі зображень за подвійним фокусом, буде дійсним, збільшеним, зворотним; якщо предмет розташований між переднім фокусом і системою, його зображення, одержуване також у просторі предметів, буде уявним, прямим і збільшеним.

Як стохастичний сигнал зображення є одними із найбільш уживаних видів інформації.

Але зображення є сигналом, який володіє, в додаток до типової інформа-

тивності, ще й візуальною інформативністю. Відповідно актуальною задачею є захист такого зображень від несанкціонованого доступу та використання. Це спричинює до використання відомих класичних методів шифрування у випадку шифрування зображень.

Алгоритм RSA є одним із найбільш уживаних промислових стандартів шифрування сигналів. На відміну від симетричного кодування, при якому процедура розшифровки легко відновлюється за процедурою шифрування і зворотньо, у схемі кодування з відкритим ключем неможливо обчислити процедуру дешифрування, знаючи процедуру шифрування. Безпека алгоритму RSA побудована на принципі складності факторизації цілих чисел. Алгоритм використовує два ключі — відкритий і секретний , разом відкритий і відповідний йому секретний ключі утворюють пару ключів.

Така інформативність із сучасними методами обробки зображень дає можливість для реалізації несанкціонованого доступу. Організація атаки на зашифроване зображення можлива у двох варіантах: через традиційний злом методів шифрування, або через методи візуальної обробки зображень (методи фільтрації, виділення контурів, тощо). В зв'язку з цим до методів шифрування у випадку їх використання стосовно зображень висувається ще одна вимога – повна зашумленість зашифрованого зображення. Це потрібно для того, щоб унеможливити використання методів візуальної обробки зображень.

Мета роботи

По відношенню до зображення актуальною задачею є таке модифіковане використання алгоритму RSA щоб:

- не зменшити криптографічну стійкість алгоритму RSA;
- забезпечити повну зашумленість зображення, з метою унеможливити використання методів візуальної обробки зображень.

Одним із шляхів створення такої модифікації є поєднання елементів алгоритму RSA і лінійних форм в програмній реалізації .

Характеристики зображення.

Існують два способи формування зображення технічними засобами: матричний (растровий)і векторний.

В основі матричного способу формування зображення лежить принцип розкладання його на елементи скінчених розмірів, як правило, у формі точки або прямокутника. Елемент зображення - піксель при матричному способі створення зображення не може мати структури, а тільки колір і/або яскравість.

Матричний спосіб створення зображення використовується у телебаченні, при передаванні зображень за допомогою факсимільних апаратів тощо. З точки зору інформаційної ємності, матричне зображення має досить значну надлишковість, тобто передається багато інформації, необов'язкової для сприйняття графічного образу. Наприклад, для створення суцільного тла, фону картини, зовсім необов'язково передавати інформацію окремо про колір та яскравість кожного пікселю фону.

Нехай задано рисунок P з ширини l і висоти h. Його можна розглядати як матрицю інтенсивностей пікселів

$$C=\begin{pmatrix} c_{1,1} & \cdots & c_{1,l} \\ \cdots & \cdots & \cdots \\ c_{h,1} & \cdots & c_{h,l} \end{pmatrix}, \qquad (1)$$

де c_{ij} – значення інтенсивності пікселя.

Під градацію яскравості звичайно приділяється 1 байт, причому 0 - чорний колір.

Задача виділення контура вимагає використання операцій над сусідніми елементами, які є чутливими до змін і пригашають області постійних рівнів яскравості, тобто, контури – це ті області, де виникають зміни, стаючи світлими, тоді як інші частини зображення залишаються темними. Тому виділення контура означає пошук найбільш різких змін, тобто максимумів модуля вектора градієнта [2]. Це є однією з причин, через що контури залишаються в зображенні при шифруванні в системі RSA, оскільки шифрування тут базується на піднесенні до степеня по модулю деякого натурального числа. При цьому, на контурі і на сусідніх до контура пікселах піднесення до степеня значення яскравостей дає ще більший розрив.

Опис алгоритму шифрування.

Шифрування по шести рядках матриці зображення.

Нехай P,Q,R,T,W,U - три пари довільних простих чисел і $N=P*Q, M=R*T$ $N=P*Q, M=R*T$, $L=W*V$, $j(N)=(P-1)(Q-1)$, $j(M)=(R-1)(T-1)$, $j(M)=(R-1)(T-1)$, $j(N)=(U-1)(W-1)$. Шифрування відбувається поелементно з використанням наступного перетворення елементів матриці зображення $\boldsymbol{C}$:

1. Випадково вибирається натуральне число $e<j(N)$ і знаходиться таке натуральне d, щоб виконувалася конгруенція $ed=1(\mathbf{mod} j(N))$.

2. Випадково вибирається натуральне число $s < j(M)$ і знаходиться таке натуральне t, щоб виконувалася конгруенція $st = \mathbf{1}(\mathbf{mod} j(M))$.
3. Випадково вибирається натуральне число $u < j(L)$ і знаходиться таке натуральне w, щоб виконувалася конгруенція $uw = \mathbf{1}(\mathbf{mod} j(L))$.
4. Для кожного $k = \mathbf{6}*i, i = \mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots$ і кожного елемента $c_{k,j}$, $\mathbf{0} \le j \le l$ будується число $bk, j = c^{e}_{(k,j)} (mod(N))$.
5. Для кожного $n = \mathbf{6}*i+\mathbf{1}, i = \mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots$ і кожного елемента $c_{n,j}$, $\mathbf{0} \le j \le l$ будується число $an, j = c^{d}_{(n,j)} (mod\ \varphi(N)) + bk, j + f(j)$, де $f(j)$ – функція зашумлення.
6. Для кожного $k = \mathbf{6}*i+\mathbf{2}, i = \mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots$ і кожного елемента $c_{k,j}$, $\mathbf{0} \le j \le l$ будується число $bk, j = c^{S}_{(k,j)} (mod(M))$.
7. Для кожного $n = \mathbf{6}*i+\mathbf{3}, i = \mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots$ і кожного елемента $c_{n,j}$, $\mathbf{0} \le j \le l$ будується число $an, j = c^{t}_{(n,j)} (mod\ \varphi(M)) + bk, j + g(j)$, де $g(j)$ – функція зашумлення.
8. Для кожного $k = \mathbf{6}*i+\mathbf{4}, i = \mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots$ і кожного елемента $c_{k,j}$, $\mathbf{0} \le j \le l$ будується число $bk, j = c^{u}_{(k,j)} (mod(L))$.
9. Для кожного $n = \mathbf{6}*i+\mathbf{5}, i = \mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots$ і кожного елемента $c_{n,j}$, $\mathbf{0} \le j \le l$ будується число $an, j = c^{w}_{(n,j)} (mod\ \varphi(L)) + bk, j + h(j)$, де $h(j)$ – функція зашумлення.

7. Зашифрованим є зображення після вибору всіх стрічок вхідного зображення.

8. Всі числа $b_{k,j}$, $a_{n,j}$ послідовно записуються в наступну матрицю

$$\boldsymbol{V} = \begin{pmatrix} b_{1,1} & \ldots & b_{1,l} \\ \ldots & \ldots & \ldots \\ b_{h,1} & \ldots & b_{h,l} \end{pmatrix}.$$

Дешифрування. Дешифрування виконується в оберненому порядку з використанням властивостей алгоритму RSA.

Результати наведені на Рис.1 – 3 при $P = \mathbf{23}, Q = \mathbf{37}, S = \mathbf{73}, T = \mathbf{37}, U = \mathbf{97}, W = \mathbf{37}$. Функції зашумлення мають вигляд - $f(j) = -j, g(j) = -j^{\mathbf{2}}, h(j) = j^{\mathbf{3}}$.

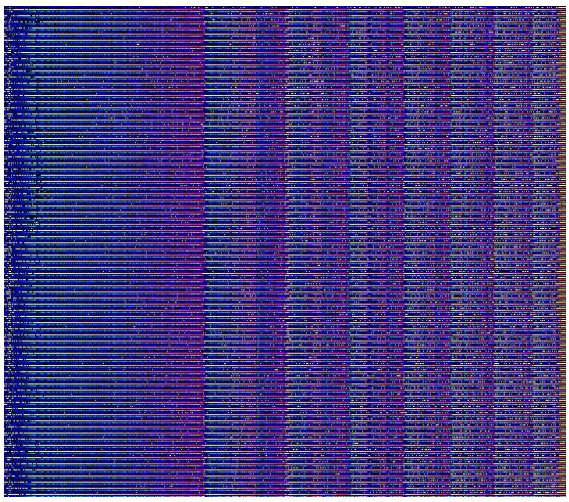

Рис.1. Початкове зображення Рис.2. Зашифроване зображення

Рис.3. Дешифроване зображення

Результати з іншим зашумленням наведені на Рис.4–6 при $P = \mathbf{43}, Q = \mathbf{37}, S = \mathbf{73}, T = \mathbf{37}, U = \mathbf{97}, W = \mathbf{37}$. Функції зашумлення мають вигляд - $f(j) = -j^{\mathbf{3}}, g(j) = -j^{\mathbf{3}}, h(j) = j^{\mathbf{3}}$.

Рис.4. Початкове зображення

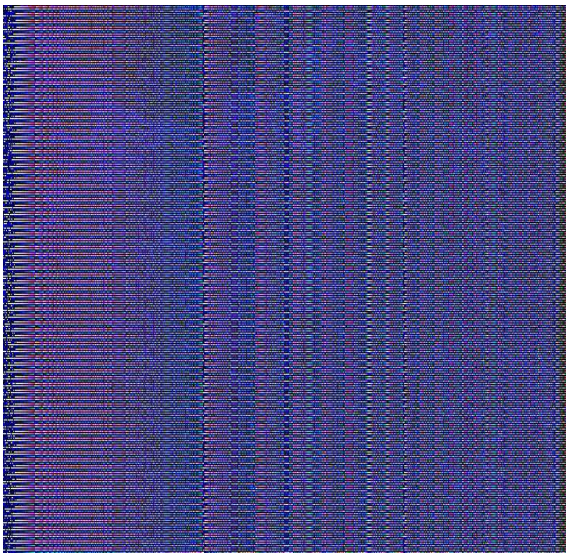

Рис.5. Зашифроване зображення

Рис.6. Дешифроване зображення

Після візуального порівняння Рис.2 і Рис.5 видно, що структура зашифрованого зображення залежить від вигляду функцій зашумлення і значень простих чисел P,Q,R,T,W,U. Контури в обох зашифрованих зображеннях відсутні. Початкове і дешифроване зображення незначно відрізняються рівнем яскравості.

Висновки

1. Запропонована модифікація шифрування може бути використана як для півтонових, так і для кольорових зображень і грунтуються на використанні ідей базового алгоритму RSA. Однак, незалежно від типу зображення, пропорційно до розмірності вхідного зображення, може зрости розмір шифрованого зображення.

2. Стійкість до несанкціонованого дешифрування запропонованого

алгоритму забезпечується стійкістю базового алгоритму RSA з додатковою стійкістю, яка надається використанням лінійних форм.

1. Павлидис Т. Алгоритмы машиной графики и обработки изображений. – М.: Радио и связь, 1986.-399с.
2. Б.Яне. Цифровая обработка изображений. – Москва, Техносфера , 2007.- 583с.
3. Брюс Шнайер. Прикладная криптография. – М.: Триумф, 2003. – 815с.
4. Ю.М. Рашкевич, Д.Д. Пелешко А.М. Ковальчук, М.З. Пелешко. Модифікація алгоритму RSA для деяких класів зображень. Технічні вісті 2008/1(27), 2(28). С. 59 – 62.
5. Ковальчук А., Пелешко Д., Борзов Ю.Бінарні операції та елементи алгоритму RSA при шифруванні – дешифруванні кольорових зображень. Комп'ютерні науки та інформаційні технології., №771, 2013, с. 121-126.

Рак Т.Е., Борзов Ю.А. Линейные формы с элементами алгоритма RSA и дополнительное зашумление в защите полутоноиых изображений.

Рассмотрены проблемы защиты изображений от несанкционированного доступа. Сформулированы требования к методам щифрования в случае их использования относительно изображений – полная зашумленность зашифрованного изображения. Описано использование элементов алгоритма RSA и линейных форм для использования при шифровании – дешифровании изображений при наличии дополнительного зашумления. Предложенная модификация базового алгоритма RSA может применяться для шифрования как для полутоновых, так и для цветных изображений. Стойкость к несанкционированному дешифрованию предложенного алгоритма обеспечивается стойкостью базового алгоритма RSA с дополнительной стойкостью, которая предоставляется использованием линейных форм.

Ключевые слова: шифрование. Дешифрование, алгоритм RSA, линейная форма.

Rak T.Ye., Borzov U.O. Linear forms with elements of the RSA algorithm and additional noise in defense of grayscale images.

This article deal with the problem of image protection from unauthorized access. The requirements to encryption methods in the case of images - full noisy encrypted image. The using of elements of the RSA algorithm and linear forms for images encrypting-deciphering in case of additional noise is described. A modification of the basic algorithm of RSA encryption can be used for grayscale and color images. Resistance to unauthorized decryption of the proposed algorithm is provided by the basic stability RSA algorithm with additional stability provided by the use of linear forms.

Keywords: encryption, decryption, the RSA algorithm, linear form.

Summary

Images, as a stochastic signal, are the most commonly used type of information. The image is a signal that has typical and visually informative. This informative combined with modern methods of image processing makes it possible to implement unauthorized access. In this regard, the encryption methods for images has another additional requirement - full noisy encrypted image. This is necessary to avoid the use of visual techniques of image processing. According urgent task is to protect this image from unauthorized access and use. This leads to the use of well-known classical encryption methods for encrypting of images.

RSA algorithm is one of the most commonly used industry standard for encryption of signals. But, it's unable to calculate decryption process in the scheme of coding of public key in case of knowing the encryption process. Security RSA algorithm is based on the principle of complexity factorization of integers. The algorithm uses two keys - public and private which form a key pair.

Organization of attacks on encrypted image is available in two versions: through traditional laying out of encryption methods or through methods of visual image processing (filtering, edge detection, etc.).

Task of allocation of contours requires the use of operations on neighboring elements, which are sensitive to changes and shade the areas of constant brightness levels, ie, contours - is those areas where there are changes, becoming lighter, while other parts of the image are dark. Therefore, the selection of contour means finding the most dramatic change - the maximum modulus of the gradient vector. This is one of the reasons that remain contours in the image when encrypting in RSA system is used, because encryption is based on exponentiation modulo of some integer. Thus, in the contour and in the neighboring pixels the exponentiation brightness value gives an even greater gap.

The actual problems of using of RSA algorithm are:

- shutting out of diminishing of resistance of cryptography of RSA algorithm;

- ensure complete noisy of image in order to prevent the use of visual techniques of image processing.

One of the ways of creating of such modification is a combination of elements of the RSA algorithm and linear forms in program implementation.

The requirements to encryption methods in the case of images - full noisy encrypted image. The using of elements of the RSA algorithm and linear forms for images encrypting-deciphering in case of additional noise is described.

A modification of the encryption can be used for grayscale and color images to and use of ideas based on the basic algorithm of RSA. However, regardless of the type of image in proportion to the dimension of the input image, the size of the encrypted image can increase.

Resistance to unauthorized decryption of the proposed algorithm provided by basic stability of RSA algorithm with additional stability provided by the linear forms.